

VILLES INTELLIGENTES : *DÉFIS TECHNOLOGIQUES ET SOCIÉTAUX*

1. Introduction
2. Infrastructures réseaux des systèmes urbains
3. Infrastructures logicielles des systèmes urbains
4. Gestion des données urbaines dans les nuages informatiques
- 5. Gestion des données et vie privée du citoyen urbain**

5. Gestion des données et vie privée du citoyen urbain

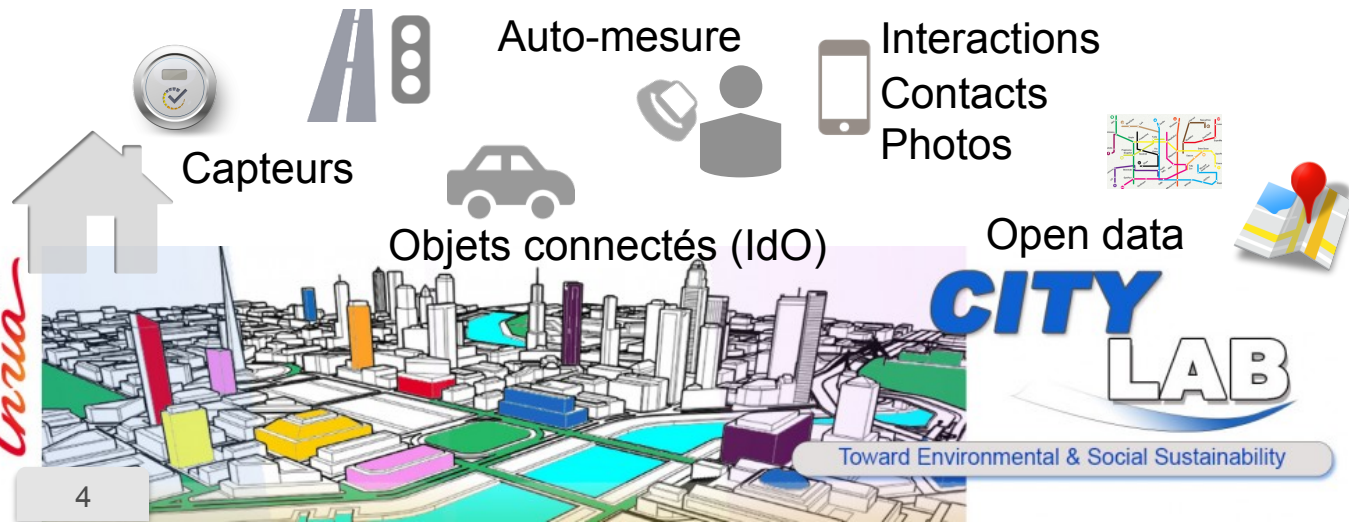
- Architectures de gestion de données face au respect de la vie privée
- Gestion de la vie privée dans les réseaux sociaux mobiles
- Privacy-by-design: gestion de données confinées (puces et capteurs)
- Gestion de la vie privée dans les applications mobiles participatives
- Traitements de données globaux respectueux de la vie privée

5. Gestion des données et vie privée du citoyen urbain

- Architectures de gestion de données face au respect de la vie privée
- Gestion de la vie privée dans les réseaux sociaux mobiles
- Privacy-by-design: gestion de données confinées (puces et capteurs)
- Gestion de la vie privée dans les applications mobiles participatives
- Traitements de données globaux respectueux de la vie privée

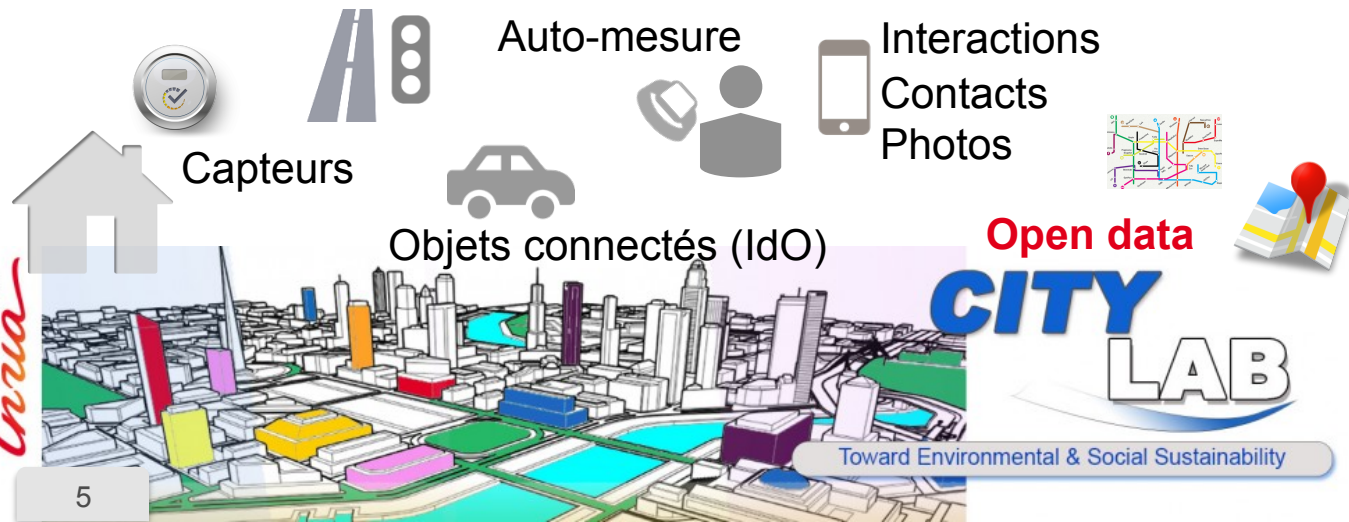
Les données dans les villes intelligentes

- Numérisation des procédés → génération massive de données personnelles
- Des données sur la ville, son activité, ses citoyens → services urbains
 - ✓ croisement de données publiques, personnelles, collectées automatiquement ou de manière participative



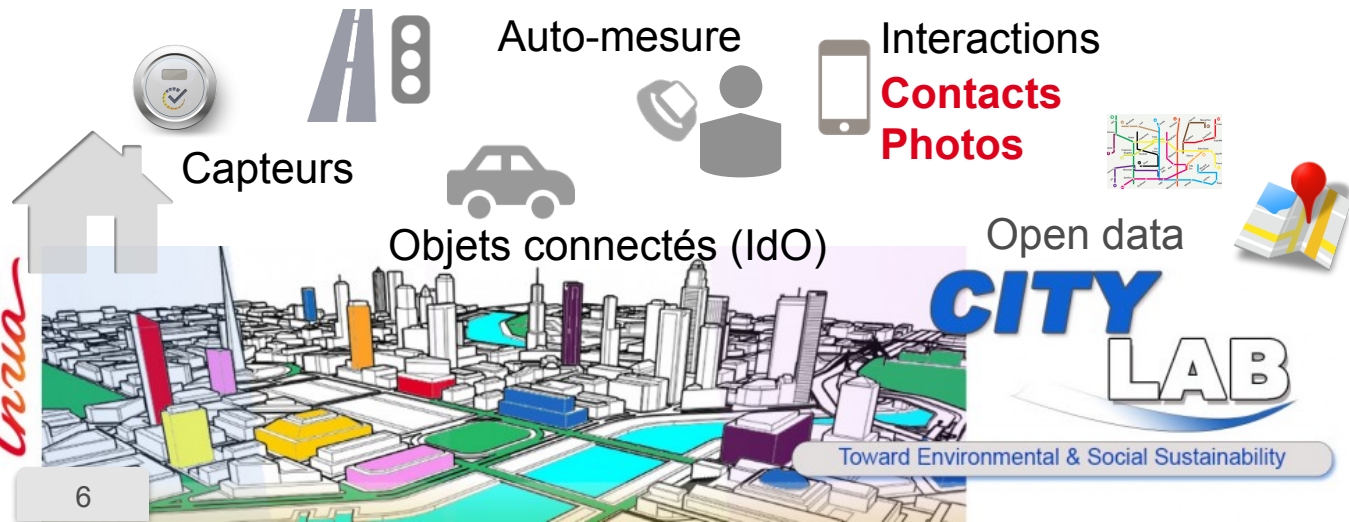
Les données dans les villes intelligentes

- Numérisation des procédés → génération massive de données personnelles
- Des données sur la ville, son activité, ses citoyens → services urbains
 - ✓ croisement de données publiques, personnelles, collectées automatiquement ou de manière participative



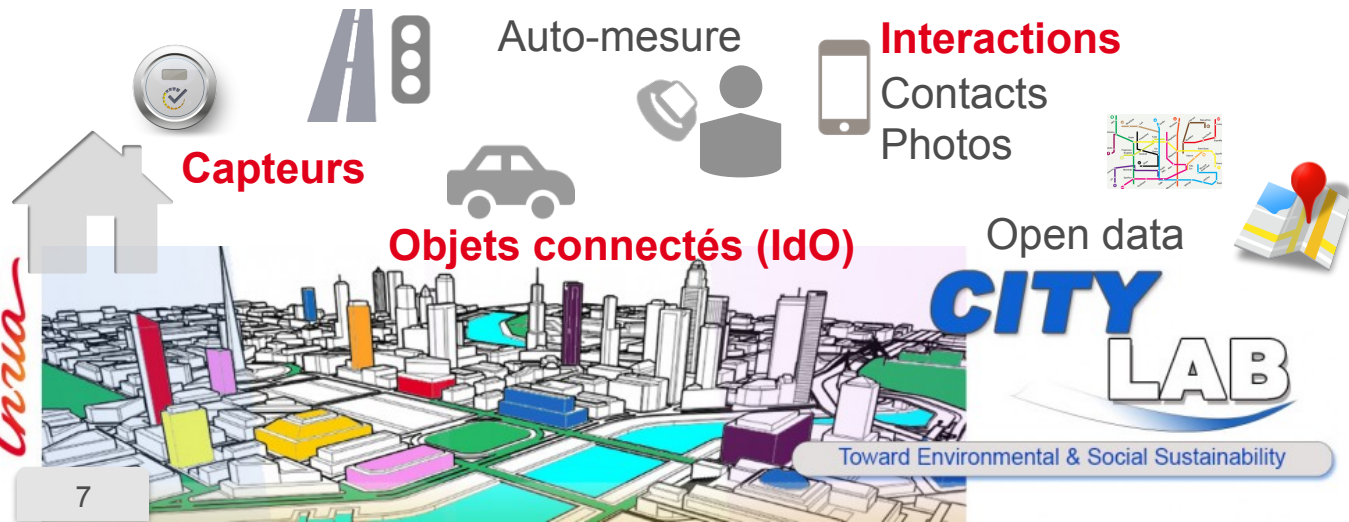
Les données dans les villes intelligentes

- Numérisation des procédés → génération massive de données personnelles
- Des données sur la ville, son activité, ses citoyens → services urbains
 - ✓ croisement de données publiques, personnelles, collectées automatiquement ou de manière participative



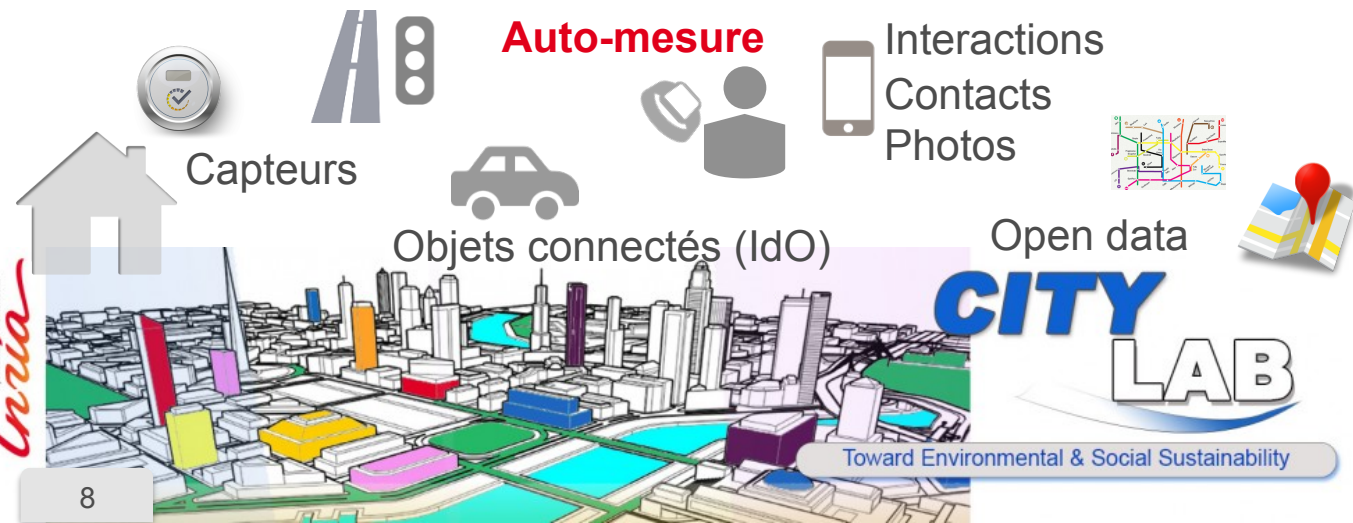
Les données dans les villes intelligentes

- Numérisation des procédés → génération massive de données personnelles
- Des données sur la ville, son activité, ses citoyens → services urbains
 - ✓ croisement de données publiques, personnelles, collectées automatiquement ou de manière participative



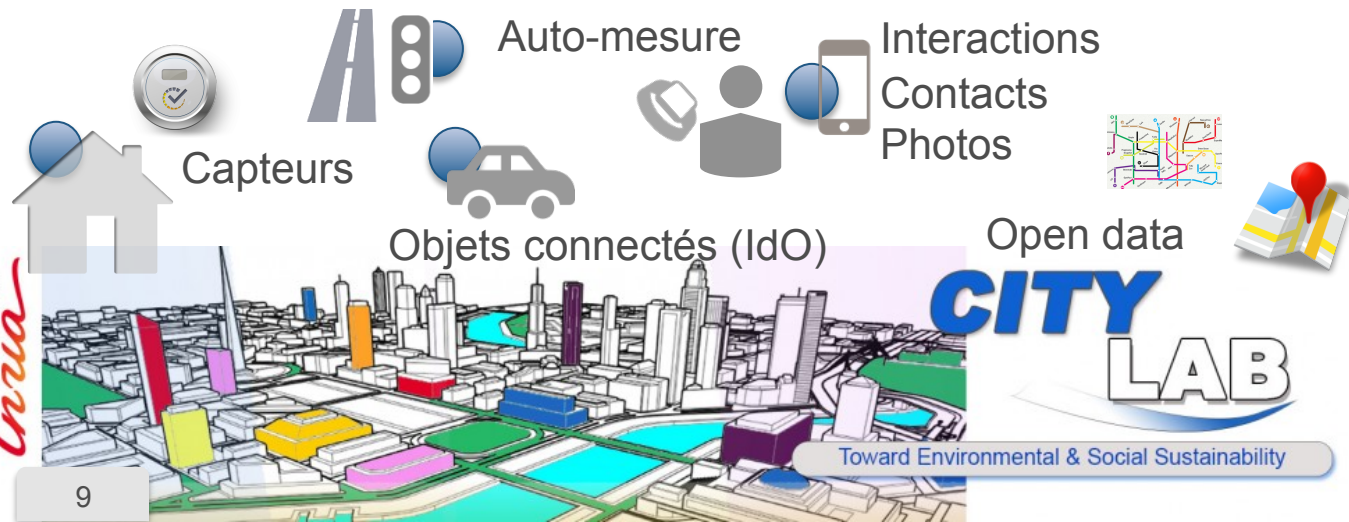
Les données dans les villes intelligentes

- Numérisation des procédés → génération massive de données personnelles
- Des données sur la ville, son activité, ses citoyens → services urbains
 - ✓ croisement de données publiques, personnelles, collectées automatiquement ou de manière participative



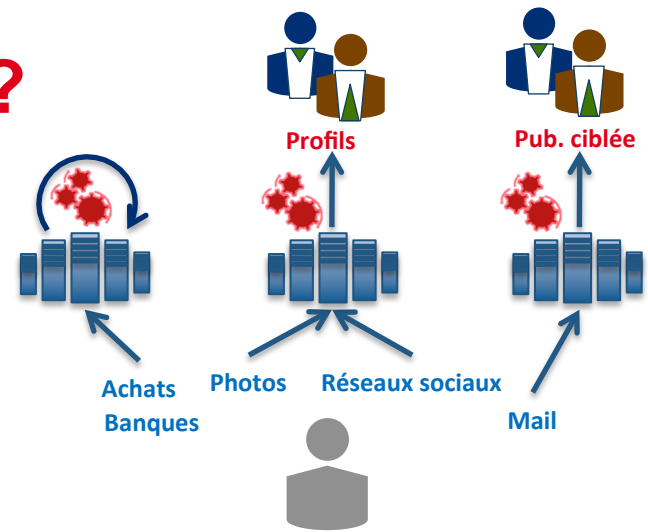
Les données dans les villes intelligentes

Comment gérer ces données dans le respect de la vie privée des citoyens urbains ?



Selon le modèle du Web actuel ?

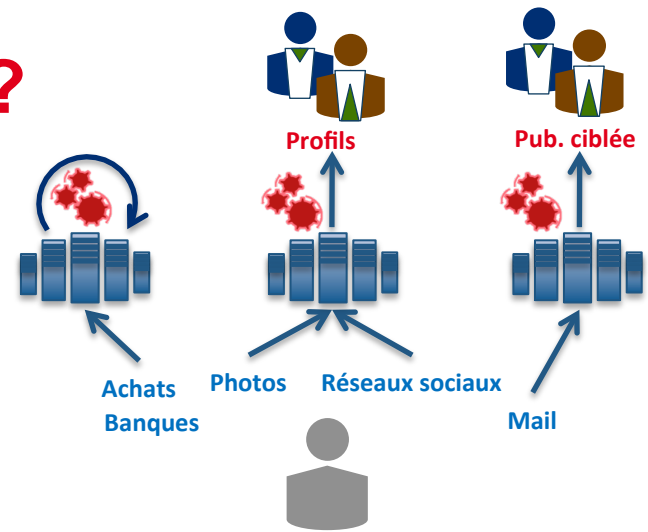
- **Délégation** → vie privée ?
- **Très grands volumes** → sécurité ?
- **Fragmentation** → complétude ?



Selon le modèle du Web actuel ?

- **Délégation** → vie privée ?
- **Très grands volumes** → sécurité ?
- **Fragmentation** → complétude ?

Consensus : donner plus de contrôle au citoyen sur ses données [WEF12]

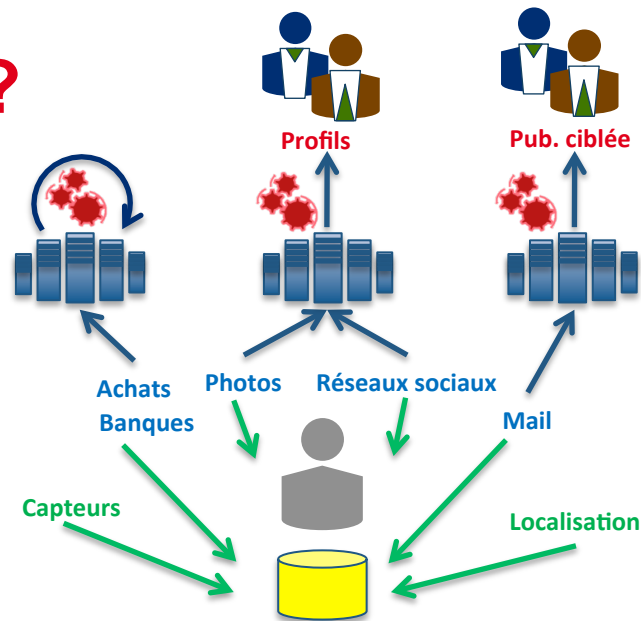


Selon le modèle du Web actuel ?

- **Délégation** → vie privée ?
- **Très grands volumes** → sécurité ?
- **Fragmentation** → complétude ?

Consensus : donner plus de contrôle au citoyen sur ses données [WEF12]

- **Web personnel** : rendre les données
 - Analyses croisées
 - Dissémination contrôlée
 - Calculs participatifs anonymes

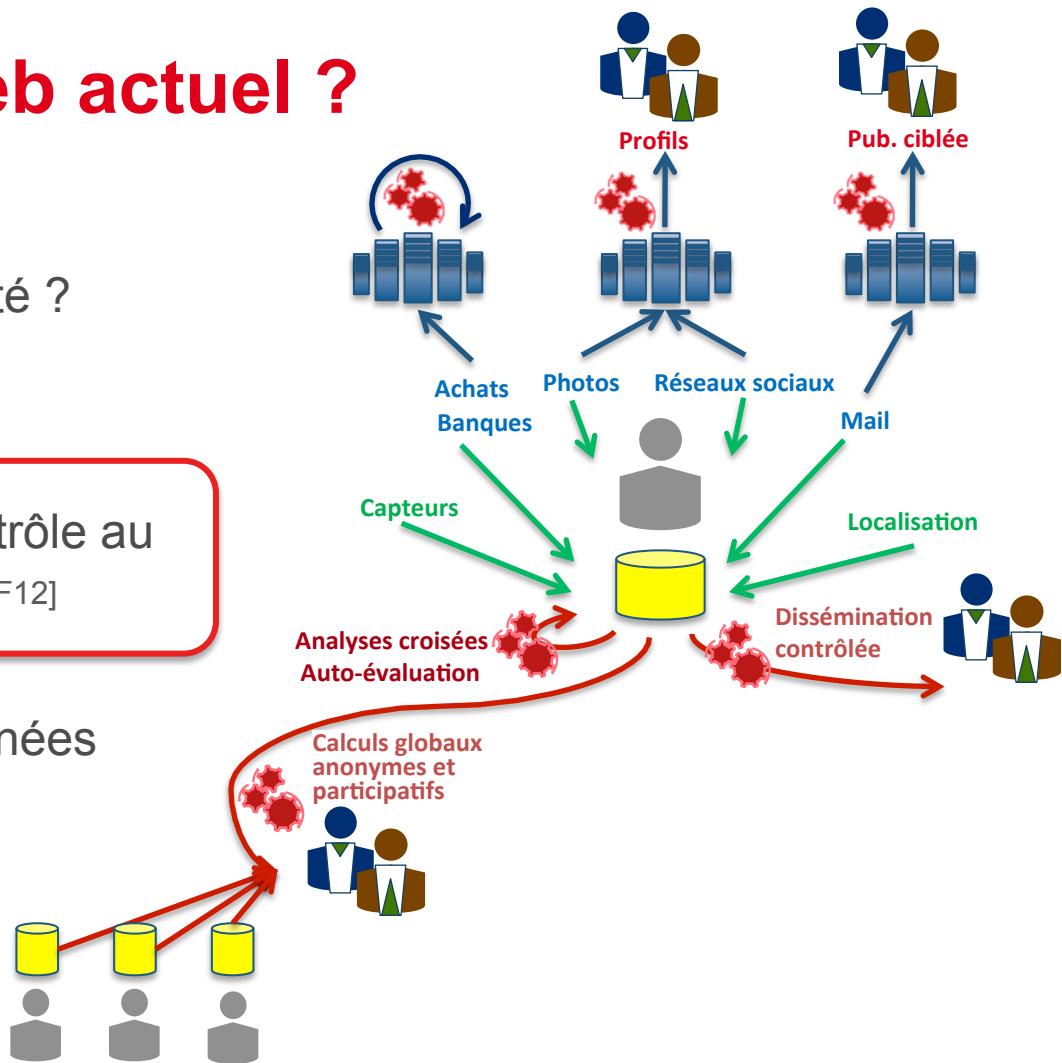


Selon le modèle du Web actuel ?

- **Délégation** → vie privée ?
- **Très grands volumes** → sécurité ?
- **Fragmentation** → complétude ?

Consensus : donner plus de contrôle au citoyen sur ses données [WEF12]

- **Web personnel** : rendre les données
 - Analyses croisées
 - Dissémination contrôlée
 - Calculs participatifs anonymes



Comment rendre ses données au citoyen ?

- **Sur son ordinateur personnel ?**
 - Auto-administration, sécurité
- **Sur un service Cloud ?**
 - Aggravation du problème sous prétexte de vie privée
- **Principes fondateurs des architectures envisagées**
 - Centrées sur l'individu, la propriété des données, et la vie privée
 - Cadre propice à la législation et aux recommandations des CNIL

Comment rendre ses données au citoyen ?

- **Solution dominante : des serveurs de confiance**

- Normes, labellisation, cadre contractuel

Ex: Cloud souverain, DB Hippocratiques (IBM), infomédiaires, VRM

- Sécurité (cryptographie, matériel résistant aux attaques)

Ex: CryptDB [SOSP11], Oracle HSM, TrustedDB [TKDE14]

- **Nouvelle approche : serveurs personnels de données**

- PDS/PlugDB@Inria [VLDB10], OpenPDS@MIT [PLOS14], CozyCloud, OwnCloud ...
- Blue Button (USA), MesInfo (FR) ...

Serveur personnel* ...

- **Chaque serveur est personnel et de confiance pour son propriétaire**
 - Le serveur d'un seul individu → pas de concentration
 - Administré par l'individu → pas de délégation

Serveur personnel* ...

- Chaque serveur est personnel et de confiance pour son propriétaire
- **Exécution locale au serveur personnel**
 - Régulation de la diffusion des données
 - Ex: OpenPDS@MIT [PLOS14]

Serveur personnel* ...

- Chaque serveur est personnel et de confiance pour son propriétaire
- Exécution locale au serveur personnel
- **+ Logiciel libre et plateforme isolée (matériel dédié ou virtualisé)**
 - Vérification communautaire, sécurité renforcée vis-à-vis des applications
 - Ex: Freedombox, Owncloud, CozyCloud, CloudMask...

Serveur personnel* ...

- Chaque serveur est personnel et de confiance pour son propriétaire
- Exécution locale au serveur personnel
- + Logiciel libre et plateforme isolée (matériel dédié ou virtualisé)
- **+ Sécurité matérielle**
 - Résistance aux attaques physiques
 - Ex: PDS/PlugDB@Inria [VLDB10]

Références

- [Cavoukian12] Cavoukian, A. (2012). Privacy by design and the emerging personal data ecosystem. *Privacy By Design*.
- [CFP00] Catlett, J. Panel on infomediaries and negotiated privacy techniques. In Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions, CFP '00, pages 155–156, New York, NY, USA, 2000
- [JDDDM08] Mitchell, A., Henderson, I. and D. Searls. Reinventing direct marketing — with VRM inside. *Journal of Direct Data and Digital Marketing Practice*, 10(1):3–15, 2008
- [PLOS14] de Montjoye, Y. A., Shmueli, E., Wang, S. S., & Pentland, A. S. (2014). OpenPDS: Protecting the privacy of metadata through safeanswers. *PloS one*, 9(7).
- [PlugDB] <https://project.inria.fr/plugdb/>
- [VLDB10] Allard, T., Anciaux, N., Bouganim, L., Guo, Y., Le Folgoc, L., Nguyen, B., ... & Yin, S. (2010). Secure personal data servers: a vision paper. *Proceedings of the VLDB Endowment*, 3(1-2), 25-35.
- [SOSP11] Popa, R. A., Redfield, C., Zeldovich, N., & Balakrishnan, H. (2011, October). CryptDB: protecting confidentiality with encrypted query processing. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles* (pp. 85-100). ACM.
- [TKDE14] Bajaj, S., & Sion, R. (2014). TrustedDB: A trusted hardware-based database with privacy and data confidentiality. *Knowledge and Data Engineering, IEEE Transactions on*, 26(3), 752-765.
- [WEF12] The World Economic Forum. Rethinking Personal Data: Strengthening Trust. May 2012
- VRM project, <http://blogs.law.harvard.edu/vrm/projects/>
- CozyCloud <https://cozy.io/fr/> ; OwnCloud <https://owncloud.org/> ; FreedomBox <http://freedomboxfoundation.org/>
- Wikipedia: Freedombox, Vendor Relationship Management